© Copyright IBM Corporation 2015

한국아이비엠주식회사

(150-945) 서울시 영등포구 국제금융로10
서울국제금융센터 (Three IFC)

TEL : (02)3781-7800
www.ibm.com/kr

2015년 7월

Printed in Korea
All Rights Reserved

IBM, IBM 로고, ibm.com은 미국 및/또는 다른 국가에서 IBM Corporation의 상표 또는 등록 상표입니다. 상기 및 기타 IBM 상표로 등록된 용어가 본 문서에 처음 나올 때 상표 기호(® 또는 ™)와 함께 표시되었을 경우, 이러한 기호는 본 문서가 출판된 시점에 IBM이 소유한 미국 등록 상표이거나 관습법에 의해 인정되는 상표임을 나타냅니다.

해당 상표는 미국 외의 다른 국가에서도 등록 상표이거나 관습법적인 상표일 수 있습니다. IBM의 최신 상표 목록은 ibm.com/legal/copytrade.shtml 웹 페이지의 "저작권 및 상표 정보" 부분에서 확인할 수 있습니다.

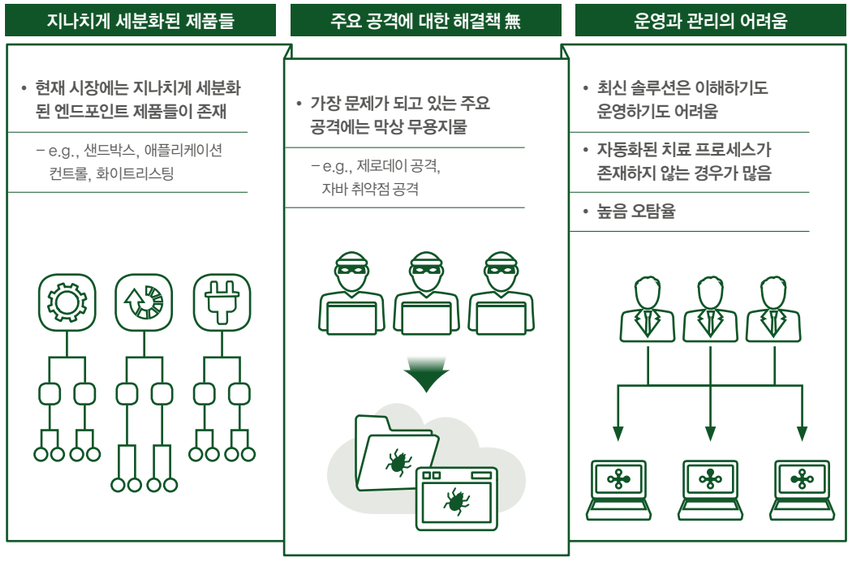
기타 다른 회사, 제품 및 서비스 이름은 다른 회사의 상표 또는 서비스 표시일 수 있습니다.

이 문서에는 IBM 제품과 서비스를 참조한 경우에도 IBM이 비즈니스를 수행하고 있는 모든 국가에서 해당 제품과 서비스를 제공함을 의미하는 것은 아닙니다.

APT 공격 대응 솔루션
IBM Trusteer Apex

APT 공격 대응 솔루션
IBM Trusteer Apex

APT 공격에 대한 현 대응 솔루션들의 한계



IBM Trusteer Apex 솔루션의 주요 기능

Trusteer Apex는 기업 및 기관의 APT 공격에 대응하기 위한 특화된 엔드포인트 보안 솔루션으로서, 이는 아래 그림 1에서 보여주는 바와 같이, 엔드포인트 내 여러 계층에서 침입을 방어하고, 적은 인력으로도 운영할 수 있는 편의성을 제공하며, 그간 수천만 개의 엔드포인트에서 수집한 다양한 공격형태를 반영하고 있습니다.

그림 1. 예방적이고 사용편의적인 엔드포인트 솔루션

Trusteer Apex 아키텍처

해커들은 공격 대상이 선정되면, 공격 컨텐츠를 전달하여 해당 기업이나 기관의 엔드포인트 상에서 취약점을 발견 및 공격하고, 악성코드를 심어 주요 정보에 접근하고 이를 통해 주요 정보를 유출하는 과정을 보입니다.

Trusteer Apex솔루션은 해커들의 일반적인 공격이 이루어지기 전에 공격 및 위험리포트를 작성하여 제공하고 개인식별정보 보호와 함께 내부 취약점을 진단/보호하고 악성파일 검사를 통해 악성코드를 잡아내고 악성통신을 차단함으로써, 내부 정보가 외부 해커로 유출되는 것을 방지하는 아키텍처를 이루고 있습니다.

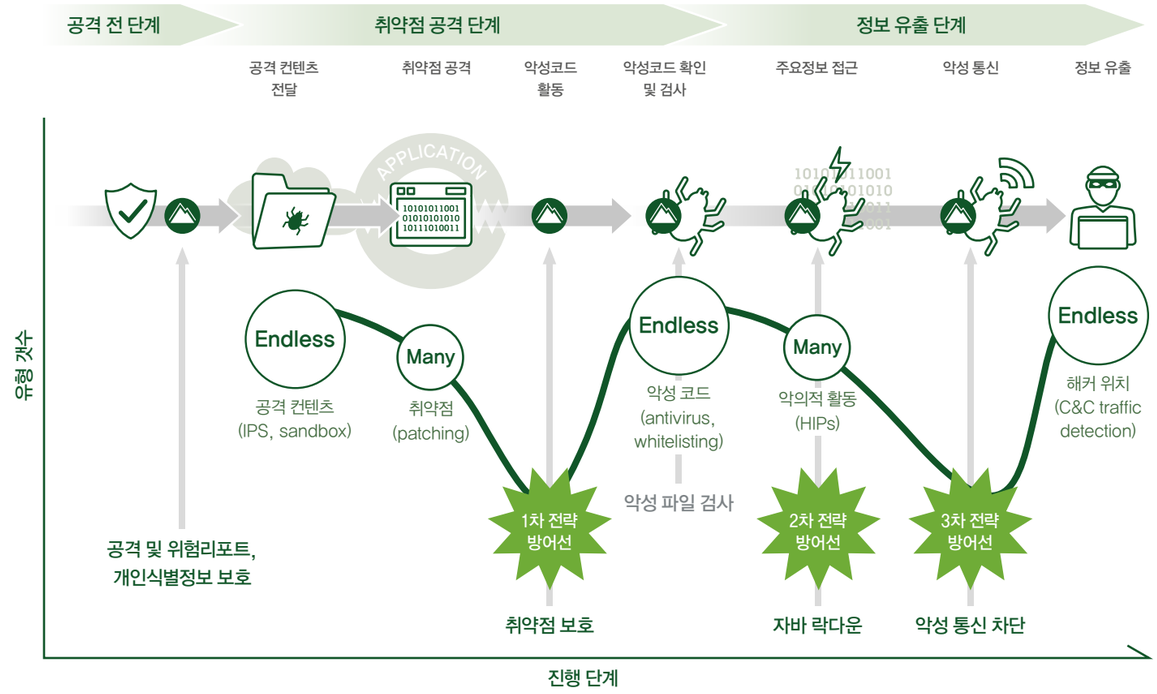


그림 2. 엔드포인트 상에서 다계층 방어선 설정 및 보호를 통한 대응 아키텍처

Trusteer Apex의 다계층 방어를 위한 핵심 기술 요소

공격 및 위험 리포트 (Threat and Risk Reporting) NEW
Vulnerability Mapping and Critical Event Reporting

포괄적 솔루션 (Advanced Threat Analysis and Turnkey Service)

❶ 개인식별정보 보호
- 개인식별정보에 대한 피싱사이트 및 비기업용 사용에 대한 경고 및 사용금지

❷ 애플리케이션 취약점 보호
- 취약점을 이용한 공격 방어
- 취약점의 주요방어 포인트를 활용한 제로데이 공격에 대한 방어

❸ 클라우드 기반 악성파일 검사 NEW
- 기존 바이러스에 대한 방어
- 27개 안티 바이러스 엔진을 통합한 검사

❹ 자바 락다운 NEW
- 자바애플리케이션의 취약점에 대한 보호

❺ 악성 통신 차단
- 악성코드 통신 차단
- 해커서버(C&C) 통신 차단 control
- 정보 유출 차단

Global Threat Research and Intelligence
Global threat intelligence delivered in near–real time from the cloud

1. 개인식별정보 보호

사내 전사 시스템 사용 시 가장 우선으로 적용해야 할 정책은 피싱사이트나 개인 사이트에 동일한 개인식별정보(비밀번호 등)를 사용하지 못하도록 하는 것입니다. Trusteer Apex는 이에 대한 정책 설정과 솔루션을 제공합니다.

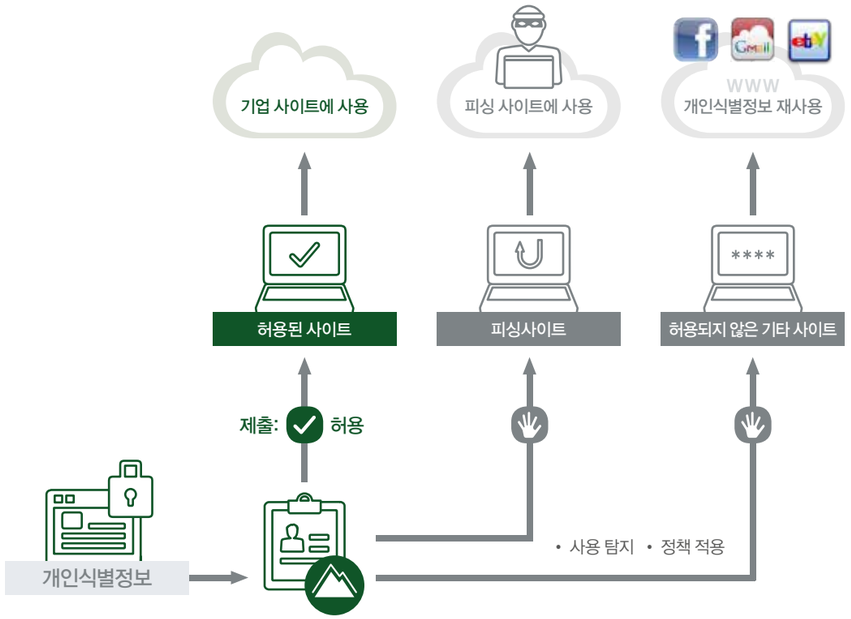


그림 3. 다계층 방어선 설정 및 보호를 통한 Trusteer Apex 대응 아키텍처

2. 애플리케이션 취약점 보호

애플리케이션의 상태에 따라 프로세스의 적합 상태를 진단하여 취약점의 공격행위를 감시하여 허용 또는 차단을 결정합니다. 이는 특정 위험 행위를 무조건적으로 막는 행위기반 방어 방법과는 구별되어, 행위의 시작의 상태를 적절히 판단하는 Trusteer Apex 만의 노하우가 들어있습니다.

- ☑ 애플리케이션 상태와 공격행위를 연계하여 상태진단
- ☑ 상태진단에 따른 행위허용 및 차단

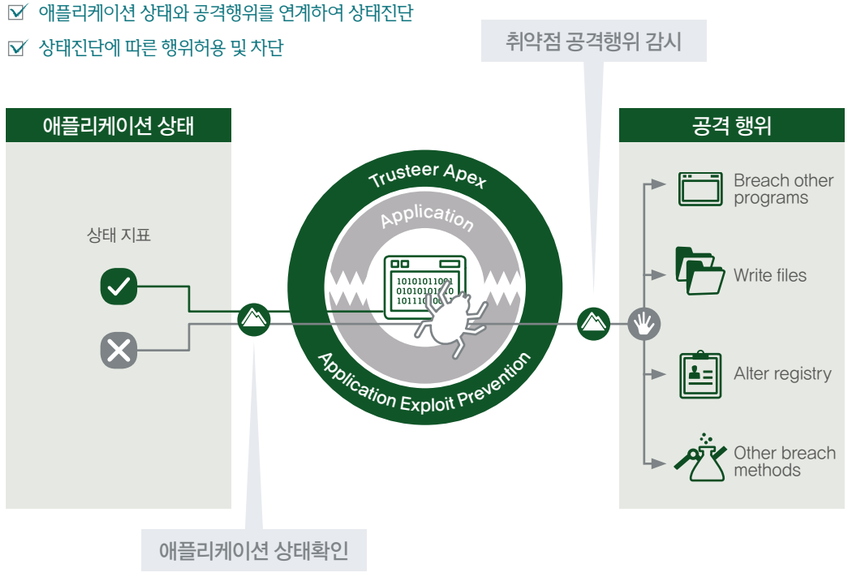


그림 4. 제로데이 공격 방어

3. 클라우드 기반 악성파일 검사

클라우드 기반의 안티바이러스로서, 네트워크에 과부하를 주는 시그니처 업데이트 없이 실시간 최신 악성코드 및 화이트리스트 정보를 적용할 수 있습니다.

- ☑ 클라우드 안티바이러스: 엔드포인트에는 시그니처 업데이트 과정이 없음
- ☑ 화이트리스트의 관리

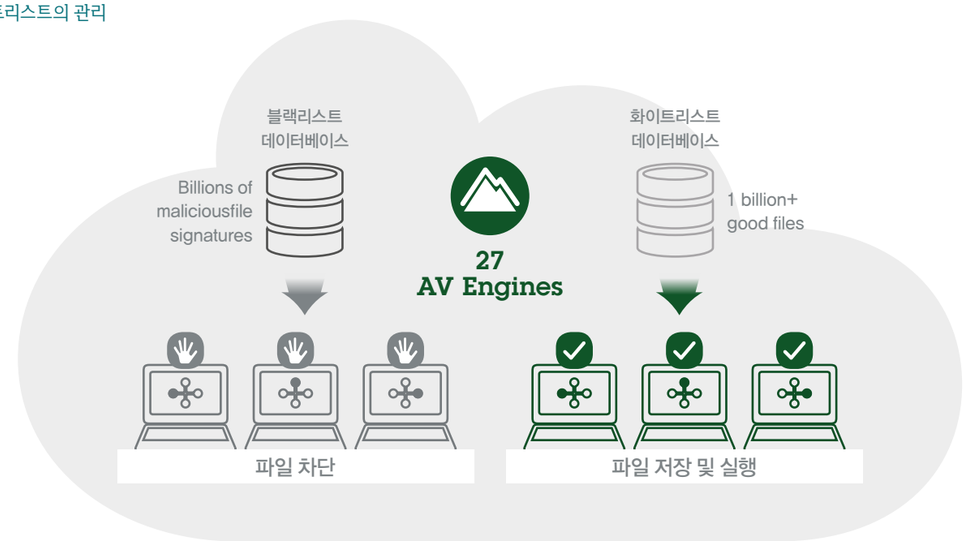


그림 5. Legacy threat protection with improved operability

4. 자바 락다운

언어의 특성 상 자바 애플리케이션의 취약점은 널리 알려져있고, 이를 이용한 공격 또한 많이 사용되고 있습니다. 따라서 Trusteer Apex는 자바 애플리케이션을 행위의 위험도 정도에 따라 모니터링 / 차단 / 적용의 솔루션을 제공합니다.

- ☑ 악성애플리케이션과 일반애플리케이션의 구분
- ☑ 트러스티어와 IT 관리자에 의한 관리

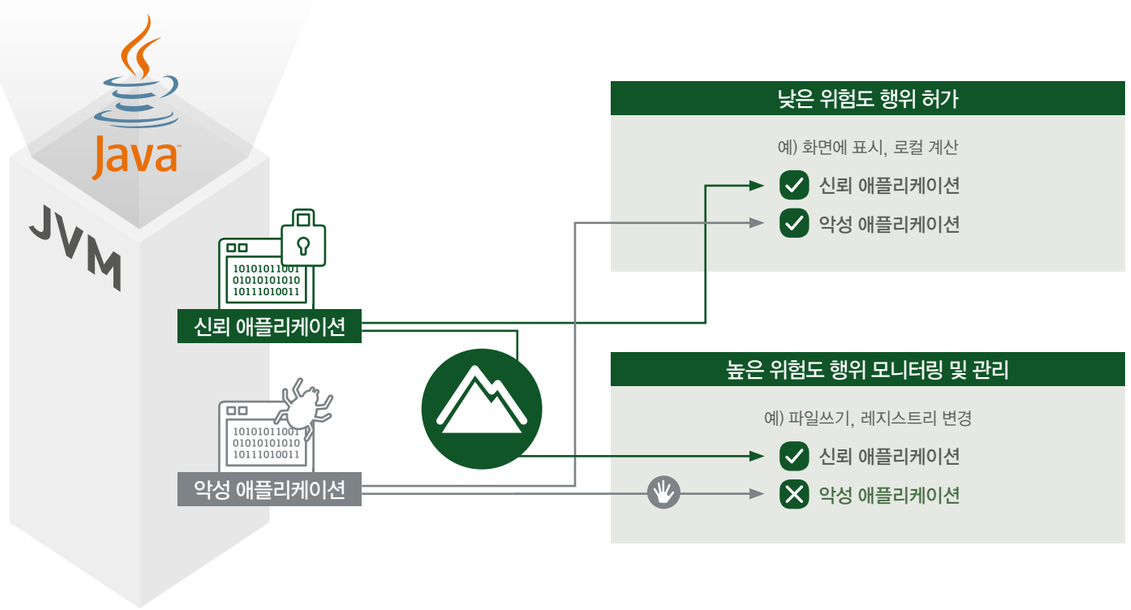


그림 6. 자바애플리케이션에 대한 모니터링과 관리

5. 악성통신 차단

외부 네트워크에서 접속하는 통신을 신뢰등급, 프로세스 형태, 해커서버의 IP등을 기반으로 판단하여 차단 또는 허용합니다.

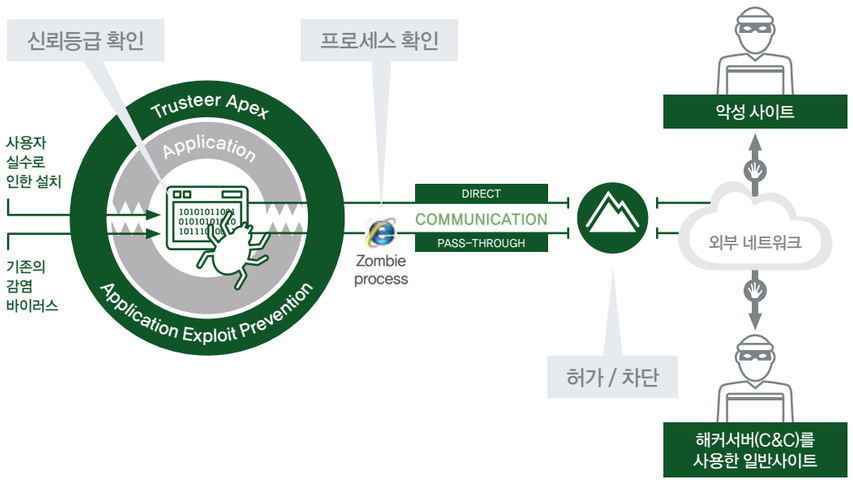


그림 7. 악성 통신 채널을 열려는 행위에 대한 차단

이와 같이 다계층 방어를 위한 IBM Trusteer Apex 솔루션은 개인식별정보 보호에서부터 악성통신 차단에 이르기까지 5가지 핵심 기술로 이루어집니다.

분석 및 인텔리전스 역량을 바탕으로 방어, 탐지, 대응의 과정으로 이루어지는 IBM의 End to End 보안 솔루션을 통해 귀사의 소중한 정보와 자산을 지키실 수 있습니다.

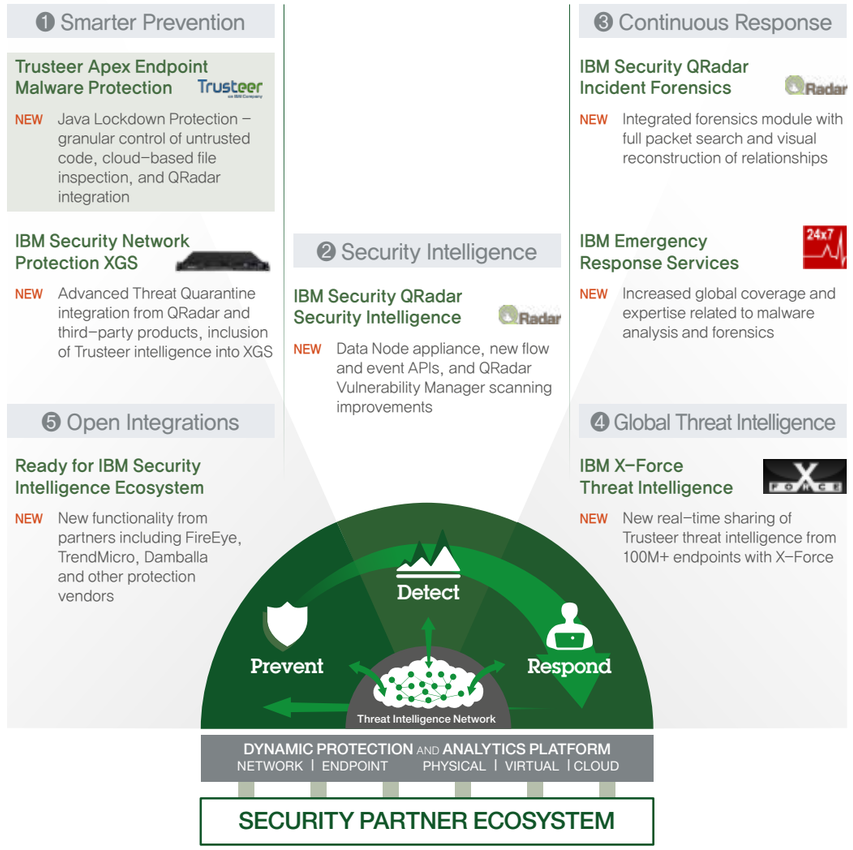


그림 8. IBM End to End 보안 솔루션